

**REMARKS**

Claims 1-32 are pending in the present application. No claims were canceled, added or amended. Reconsideration of the claims is respectfully requested.

**I. 35 U.S.C. § 102, Anticipation, Claims 1-32**

The Examiner has rejected claims 1-32 under 35 U.S.C. § 102 as being anticipated by Zhang et al. (USPN 6,553,409). This rejection is respectfully traversed.

As to claims 1-32, the Office Action states:

Regarding claims 1, 14, 17, and 30, Zhang et al. (USPN 6,553,409) teach a system for managing data in a network data processing system with means for:

- a. Receiving a packet containing data associated with content (column 6, lines 18-21).
- b. Determining whether the packet is enabled for content distribution by examining the data packet (column 6, lines 31-41). Note that in the reference, information in the packets is checked, and based on this information, it is determined if the packets will be sent on. If they have the information, they are enabled for content distribution.
- c. Responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check (column 6, lines 42-49).

Office Action dated December 22, 2004, page 2.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). The Zhang reference cited by the Examiner does not anticipate the present invention as recited in claim 1, because Zhang fails to teach each and every element of claim 1. Independent claim 1,

which is representative of independent claims 14, 17 and 30, with regards to similarly recited subject matter, recites:

1. A method in a data processing system for managing data in a network data processing system, the method comprising:
  - receiving a packet containing data associated with content;
  - determining whether the packet is enabled for content distribution by examining the data packet; and
  - responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check.

Independent claim 1 recites the feature of “determining whether the packet is enabled for content distribution by examining the data packet.” Zhang does not teach or suggest this feature. The Examiner points to column 6, lines 31 through 41, as teaching this feature:

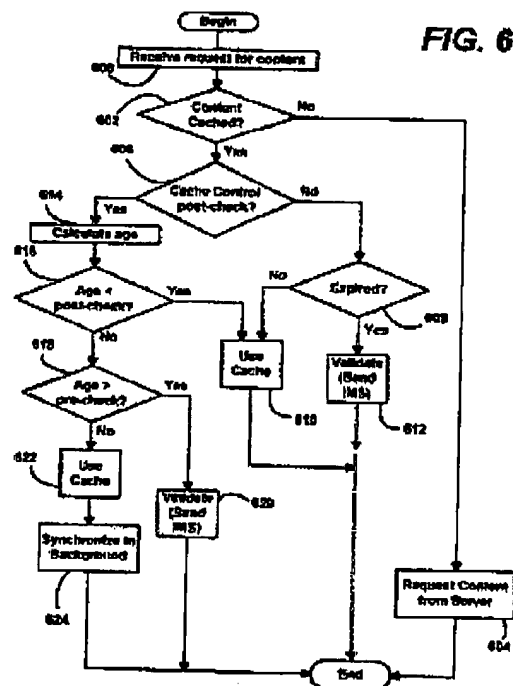
The pre-check header extension 80 and the post-check header extension 78 can be added to a normal HTTP header. For example, in FIG. 3, the pre-check header extension 80 and the post-check header extension 78 may be added to a cache control header 74 that also includes the expires header 76. In one implementation, the existence of the post-check header extension 78 and the pre-check header extension 80 overrides the use of the expires header 78. When no post-check header extension and/or pre-check header extension are present, the expires header 78 may be utilized, as described below.

The above cited passage does not teach the feature of “determining whether the packet is enabled for content distribution by examining the data packet.” Instead, the above cited passage teaches using pre-check and post-check header extensions in addition to the expires header in the cache control header. The purpose of pre-check and post-check header extensions is explained in Zhang column 6, lines 18 through 26:

In accordance with one aspect of the present invention, when present in an HTTP header, the post-check header extension 78 defines a time after which an entity/resource (e.g., the content) is to be checked for freshness. As will be described in further detail below, the check for freshness may occur in the background (background synchronization), and

occurs after the content from the cache 70 has been used. The pre-check header extension 80 defines a time after which an entity is to be checked for freshness, prior to using the entity.

The above cited passage of Zhang teaches that the post-check and pre-check header extensions define when a resource is to be checked for freshness. Determining when to refresh, or validate, data is making a validity check. This process is explained more fully by Zhang column 8, lines 59 through column 9, line 65 and Figure 6, reproduced below for the Examiner's convenience:



Turning now to an explanation of the operation of the present invention, FIG. 6 represents a general overview of a process for determining synchronization and source of requested content in accordance with one aspect of the present invention. In FIG. 6, the example of the post-check, pre-check and expires header is described herein, however it may be readily appreciated that alternative states, criteria and so forth may be tested for and applied as appropriate. Beginning at step 600, when a request for content is received, the cache manager 66 first looks to see at step 602 if the requested content is in the

cache 70. The requested content may be in the cache 70 from a prior content download, or could be available in the cache by alternative means, such as via a multicast protocol or CD-ROM installation, for example. If the requested content is not available, step 602 branches to step 604 wherein the request is otherwise handled, i.e., the request is sent to the server to retrieve the content.

If instead at step 602 the requested content is in the cache 70, step 602 branches to step 606 which determines if the requested content within the cache includes the post-check cache-control header 78 (and/or alternatively, the pre-check header). If not, step 606 branches to step 608 wherein a determination is made if the requested content within the cache 70 is expired, such as by evaluating the information within the expires header 76, for example. If the content within the cache 70 has not expired, step 608 branches to step 610 wherein the user receives the content within the cache 70 (e.g., content is rendered). If the content within the cache 70 has expired, step 608 branches to step 612 to validate the content via an DMS request or the like (or simply request new content).

However, if at step 606 the post-check cache-control header 78 is found to be present, step 606 branches to step 614 where the age of the content within the cache 70 is calculated. As stated above, a number of different criteria (parameters) can be used to determine when and if background synchronization is to occur. In the present example, the age of the content within the cache 70 is compared relative to the present request, and the determination of whether background synchronization is to occur is based upon that age. To determine the age, the time that the content within the cache 70 was retrieved is subtracted from the time of the present request, and the result is converted, as necessary, to a selected unit (e.g., seconds).

After the age is calculated, at step 616 the age of content within the cache 70 is compared against the parameter defined for the post-check header 78 (in the example shown in FIG. 3, 900 seconds). If the age is less than the parameter for the post-check header 78, step 616 branches to step 610 wherein the user receives the content within the cache 70 (e.g., content is rendered therefrom). If, however, the age is greater than the parameter for the post-check header 78, then step 616 branches to step 618 wherein the age is compared to the parameter for the pre-check header 80. An appropriate action can be defined for the unlikely event that the age equals the parameter for the post-check header 78, e.g., step 616 branches to step 618.

If the age of the content within the cache 70 is greater than the parameter for the pre-check header 80 (in the example shown in FIG. 3, 3600 seconds), then step 618 branches to step 620, where the content is

then appropriately handled, e.g., validated via an IMS request or the like. In this event, the IMS request occurs in the foreground, i.e., content is not provided to the user until a response to the IMS request is received, i.e., a "not modified" response, or (at least part of) the new content.

In accordance with one aspect of the present invention, if however, the age of the content within the cache 70 is less than the parameter for the pre-check header 80, then step 618 branches to step 622 wherein the user receives the content within the cache 70 (e.g., content is rendered). In addition, at step 624, a request for background synchronization of content is output, e.g., queued.

The above cited text and figure teaches how the post-check, pre-check and expires headers and header extensions are used to define times during which synchronized background refreshing, or validating, of the data received and stored by the cache, as well as when the data must be validated by the cache before use.

The post-check header extension defines a time after which the content should be validated in the background. So, for example, if the post-check header extension was twenty minutes, then if the cache received a request for the data twenty minutes or more after the data is received by the cache, the cache performs a validity check and returns the result that the current data is valid to use but should be refreshed in the background. That is, the cache will go ahead and return the present data to the requestor while at the same time inquiring to the source, via an IMS (If-Modified-Since) or similar query, to confirm that the data is still current.

The pre-check header extension defines a time after which data should be refreshed before sending it in response to a request. So, every time a request is received to access data, the data is checked to see how old it is, that is, how long it has been since the cache received the data. If the cache received the data longer ago than the pre-check header extension amount, then the cache will send a query to the source of the data to refresh the data before sending the data in response to the request. So, in case where the pre-check header extension is thirty minutes and a request is received for the data thirty or more minutes after the cache had received the data, the cache would first send a request to the source server to refresh the data before sending the data in response to the request.

Therefore, Zhang teaches, through the use of the pre-check and post-check header extensions, a method for determining the validity of data received and stored by a cache based on the time that has passed since the data was received by the cache. Zhang does not teach or suggest the feature of "determining whether the packet is enabled for content distribution by examining the data packet."

Additionally, claim 1 recites the feature of "responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check." Zhang does not teach or suggest this feature. The Examiner points to column 6, lines 42 through 49 as teaching this feature:

In the HTTP implementation, the post-check header extension 78 and the pre-check header extension 80 are used to set the boundaries of three distinct time periods relative to the cached content's age, wherein one period specifies when background synchronization occurs. As exemplified in FIG. 4, in a "non-validate" period, (e.g., the cached content is zero to 15 minutes old), content from the cache 70 is used, and no synchronization is requested.

The above cited passage teaches that the post-check and pre-check header extensions establish time period boundaries that determine what happens when a validity check is made by the cache. The process is more fully described in column 8, lines 59 through column 9, line 65 and Figure 6, cited above. The passage cited above teaches making validity checks, wherein three different results are returned, depending on the timing of the request relative to the post-check and pre-check header extensions. According to Zhang's example, if a request for data is received by the cache between zero to 15 minutes after the cache receives content, that is, in a time period less than that specified by the post-check header extension, the validity check returns a result that the data is valid and can be used from the cache and that no IMS request is required. If a request is received the cache after the time determined by the post-check header extension but before the time determined by the pre-check header extension, the validity checks returns a result that the data is valid and can be used from the cache, but that synchronization should occur in the background. Therefore, the data is returned from the cache to the requestor while an IMS request is sent in the back ground to refresh the data. In the case

where a request for the data is received by the cache at time after the time determined by the pre-check header extension, the validity check returns a result that the data needs to be validated by the original source before it can be sent to the requestor, and an IMS request is then sent to the originator of the data. Once a response validating the data is received by the cache, the cache then sends the validated data to the requestor.

It is important to note the difference between a validity check and validating information. Validating information means sending an IMS or equivalent request directly to the original resource in order to return the most current version of the data. In contrast, a validity check is determining if the data is current. Therefore, checking to see if the data is current, as taught in Zhang in column 8, lines 59 through column 9, line 65 and Figure 6, cited above, is making a validity check.

As the above described process, taught by Zhang, teaches making validity checks to determine if data should be used from the cache or refreshed first, it follows that Zhang cannot teach the feature of "responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check," as recited in claim 1 of the present invention.

Therefore, for all the reasons stated above, Applicants submit that independent claims 1, 14, 17, and 30 are patentable over the Zhang reference because the Zhang reference does not anticipate the present invention as recited in claims 1, 14, 17, and 30, because Zhang fails to teach and every element of claims 1, 14, 17, and 30.

Additionally, independent claim 8, 15, 24 and 31 recite features similar to those of independent claims 1, 14, 17 and 30. Specifically, independent claims 8, 15, 24 and 31 recite the feature of "responsive to a determination that the particular indicator is present, sending the content to the requestor without performing a validity check." Zhang does not teach or suggest this feature. The Examiner points to column 6, lines 42 through 49, cited above, as teaching this feature. As discussed above regarding claim 1, column 6, lines 42 through 49 teaches that the post-check and pre-check header extensions establish time period boundaries that determine what happens when a validity check is made by the cache. The process is more fully described in column 8, lines 59 through column 9, line 65 and Figure 6, also cited and discussed above.

As described above, Zhang teaches making validity checks to determine if data should be used from the cache or refreshed first. Therefore, it follows that Zhang cannot teach the feature of "responsive to a determination that the particular indicator is present, sending the content to the requestor without performing a validity check," as recited in claims 8, 15, 24 and 31 of the present invention.

Therefore, for all the reasons stated above, Applicants submit that independent claims 8, 15, 24 and 31 are patentable over the Zhang reference because the Zhang reference does not anticipate the present invention as recited in claims 8, 15, 24 and 31, because Zhang fails to teach and every element of claims 8, 15, 24 and 31.

Similarly, independent claim 13, 16, 29 and 32 recite features similar to those of independent claims 1, 14, 17 and 30. Specifically, independent claims 13, 16, 29 and 32 recite the feature of "adding an indicator and control information used to cache the content in a header of a data packet, wherein the indicator is used by an enabled node to distribute the content without performing a validity check on the content." Zhang does not teach or suggest this feature. The Examiner points to column 6, lines 42 through 49, cited above, as teaching this feature. As discussed above regarding claim 1, column 6, lines 42 through 49 teaches that the post-check and pre-check header extensions establish time period boundaries that determine what happens when a validity check is made by the cache. The process is more fully described in column 8, lines 59 through column 9, line 65 and Figure 6, also cited and discussed above.

As described above, Zhang teaches making validity checks to determine if data should be used from the cache or refreshed first. Therefore, it follows that Zhang cannot teach the feature of "adding an indicator and control information used to cache the content in a header of a data packet, wherein the indicator is used by an enabled node to distribute the content without performing a validity check on the content," as recited in claims 13, 16, 29 and 32 of the present invention.

Therefore, for all the reasons stated above, Applicants submit that independent claims 13, 16, 29 and 32 are patentable over the Zhang reference because the Zhang reference does not anticipate the present invention as recited in claims 13, 16, 29 and 32, because Zhang fails to teach and every element of claims 13, 16, 29 and 32.



Claims 2-7 are dependent claims depending from claim 1. Claims 9-12 are dependent claims depending on claim 8. Claims 18-23 are dependent claims depending from claim 17. Claims 25-28 are dependent claims depending on claim 24. As Applicants have already shown that independent claim 1, 8, 13-17, 24 and 29-32 are patentable over the Zhang reference, Applicants submit that dependent claims 2-7, 9-12, 18-23 and 25-28 are also patentable over the Zhang reference at least virtue of depending from an allowable claim.

Therefore, the rejection of claims 1-32 under 35 U.S.C. § 102 has been overcome.

Furthermore, Zhang does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. Zhang actually teaches away from the presently claimed invention because it teaches making a validity check before distributing content, as opposed to distributing distribution enabled content without making a validity check, as in the presently claimed invention. Absent the Examiner pointing out some teaching or incentive to implement Zhang and distributing distribution enabled content without making a validity check, one of ordinary skill in the art would not be led to modify Zhang to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify Zhang in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

## **II. 35 U.S.C. § 102, Anticipation, Claims 1, 3-6, 14, 17, 19-22, and 30**

The Examiner has rejected claims 1, 3-6, 14, 17, 19-22, and 30 under 35 U.S.C. § 102 as being anticipated by Taylor et al. (USPN 6,728,885). This rejection is respectfully traversed.

As to claims 1, 3-6, 14, 17, 19-22, and 30, the Office Action states:

Regarding claims 1, 14, 17, and 30, Taylor et al. (USPN 6,728,885) teach a system for managing data in a network data processing system with means for:

- a. Receiving a packet containing data associated with content (column 5, lines 39-44).
- b. Determining whether the packet is enabled for content distribution by examining the data packet (column 6,

lines 13-25). Note that in the reference, information in the packets is checked, and abased on this information, it is determined if the packets will be sent on. If they have the information, they are enabled for content distribution.

- c. Responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check (column 6, lines 31-43; column 12, lines 33-34).

Office Action dated December 22, 2004, pages 5-6.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). The Taylor reference cited by the Examiner does not anticipate the present invention as recited in claim 1, because Taylor fails to teach each and every element of claim 1. Independent claim 1, which is representative of independent claims 14, 17 and 30, with regards to similarly recited subject matter, recites:

1. A method in a data processing system for managing data in a network data processing system, the method comprising:
  - receiving a packet containing data associated with content;
  - determining whether the packet is enabled for content distribution by examining the data packet; and
  - responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check.

Independent claim 1 recites the feature of "determining whether the packet is enabled for content distribution by examining the data packet." Taylor does not teach or

suggest this feature. The Examiner points to column 6, lines 13 through 25, as teaching this feature:

In step 311, to be performed when the port is registered, DPF 207 transfers attribute information of the packet to proxy 211. Preferably, the attribute information includes the source and destination addresses of the packet and the port on which the packet was received. It should be noted, however, other information contained the connection establishing packet can be sent to proxy as well. Once the attribute information has been sent to proxy, DPF 207 awaits instructions therefrom.

The above cited passage teaches sending attribute information from a firewall to a proxy regarding a packet that is trying to establish a connection. This type of packet is known as a connection control packet, which is explained in column 5, lines 39 through 43:

Referring to FIG. 3, in step 253, DPF 207 determined whether the received packet is a connection control packet which requests to establish a data communication connection, disconnect an established connection, or put an established connection into a hold state.

Connection control packets and data packets are different types of packets, as explained in column 1, lines 47 through 54:

Further, the plurality of packets from the file includes a plurality of connection control packets and data transfer packets. The connection control packets include at least one connection establishing packet, e.g., a SYN packet, and at least one connection disconnection packet, e.g., RST, FIN, FIN-ACK packets. The data transfer packets include the pieces of the broken up file.

Therefore, as data packets and connection control packets are different entities, and since column 6, lines 13 through 25 of Taylor specifically teaches passing attribute information for connection establishing packets, it follows that Taylor does not teach the feature of "determining whether the packet is enabled for content distribution by examining the data packet."

Additionally, claim 1 recites the feature of "responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check." Taylor does not teach or suggest this feature. The Examiner cites to two passages, column 6, lines 31 through 43 and column 12, lines 33 through 34 as teaching this feature:

Another dynamic filter rule is a selective filtering rule. This rule requires proxy 211 to handle connection control packets and packet filters to handle the data packets. In other words, the packet filtering will be enabled only when proxy 211 has performed its security checks for the connections, i.e., checking the relevant information on the SYN packet sent by DPF 207. For instance, this rule is useful for protocols such as File Transfer Protocol (FTP), which sends data packets on a different connection after establishing the connection. Other filtering rules are also possible such as not applying any filtering or applying a proxy filter at the application layer to all packets received on a specific connection.

Column 6, lines 31-43

and if no user specified rule matches the packet, the packet is sent to its destination (step 339).

Column 12, lines 33-34

The above cited passage, column 6, lines 31 through 43 of Taylor does not teach the feature of "responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check." Instead, the passage teaches that one type of filtering that can be used by firewalls is dynamic filtering. In the case of dynamic filtering, packet filters filter data packets only after the proxy has performed its security checks, which means checking the relevant information on the SYN packet sent by the Dynamic Packet Filter module (DPF). A SYN packet is a connection control packet that is a connection establishing packet. After the security check is done then packet filters filter the data packets.

Nowhere does Taylor teach that the filtering done by the packet filters is done in response to the packet being enabled for content distribution. Instead Taylor teaches that packet filtering is done in response to a security check being made. Therefore, Taylor

does not teach the feature of “responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check.”

Additionally, Taylor teaches filtering data packets, not “distributing the content in response to a request for the content without requiring a validity check,” as recited in claim 1. Filtering is not distributing. Also, the filtering is done after, or in response to, a security check performed on a different type of packet, a connection control packet. This is not the same as “distributing the content in response to a request for the content without requiring a validity check.” Therefore, Taylor does not teach the feature of “distributing the content in response to a request for the content without requiring a validity check.”

The above cited passage, column 12, lines 33-34 of Taylor does not teach the feature of “responsive to the packet being enabled for content distribution, distributing the content in response to a request for the content without requiring a validity check.” Instead, the above cited passage teaches that the packet is allowed to continue on to its destination if it does not match any user specified rule. User specified rules “include user specified static filter rules and user specified dynamic filter rules.” (Taylor, Column 11, lines 10-11). Taylor, in column 10, line 62 through column 11, line 6, teaches that:

Whether the packet matches a user specified rule is determined by attribute information of the packet. The attribute information of the packet includes:

Source and destination computer addresses;

Source and destination transport layer protocol numbers;

Type of protocol (TCP, UDP etc.); and

Port numbers of NIC 203 on which the packet was received.

Anyone or a combination of the attributes can be utilized to determine if the packet matches with any user specified rules.

Therefore, Taylor teaches that whether or not a packet is allowed to continue on to its destination is determined by one or more of the above cited attributes. This is different

than “distributing the content in response to a request for the content without requiring a validity check,” as recited in claim 1. Thus, Taylor does not teach “distributing the content in response to a request for the content without requiring a validity check.”

Therefore, for all the reasons stated above, Applicants submit that independent claims 1, 14, 17, and 30 are patentable over the Taylor reference because the Taylor reference does not teach or suggest the presently claimed invention.

Claims 3-6 are dependent claims depending from claim 1. Claims 19-22 are dependent claims depending from claim 17. As Applicants have already shown that independent claim 1, 14, 17, and 30 are patentable over the Taylor reference, Applicants submit that dependent claims 3-6 and 19-22 are also patentable over the Taylor reference at least virtue of depending from an allowable claim. Additionally, claims 3-6 and 19-22 claim other additional combinations of features not taught or suggested by Taylor.

For example, claims 3 and 19 recite the feature of “responsive to an absence of an enablement for content distribution, performing a validity check on the content in response to a request for the content.” Taylor does not teach this feature. The Examiner points to column 6, lines 45 through 50 as teaching this feature:

For example, packets received from a particular port can be subjected to the filter all rule filter, while packets received from another port can be subjected to the selective filtering rule.

The above cited passage does not teach the feature of “responsive to an absence of an enablement for content distribution, performing a validity check on the content in response to a request for the content.” Instead, the above cited passage teaches that different filter rules can be applied to packets based on what physical port they came from. The above cited passage makes no mention of “performing a validity check,” nor of “performing a validity check on the content in response to a request for the content.” Therefore, Taylor does not teach the feature of “responsive to an absence of an enablement for content distribution, performing a validity check on the content in response to a request for the content,” as recited in claims 3 and 19 of the present invention.

Therefore, the rejection of claims 1, 3-6, 14, 17, 19-22, and 30 under 35 U.S.C. § 102 has been overcome.

Furthermore, Taylor does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. Taylor actually teaches away from the presently claimed invention because it teaches a DPF gathering attribute information about a connection control packet, as opposed to determining whether a packet is enabled for content distribution by examining the data packet, as in the presently claimed invention. Absent the Examiner pointing out some teaching or incentive to implement Taylor and determining whether a packet is enabled for content distribution by examining the data packet, one of ordinary skill in the art would not be led to modify Taylor to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify Taylor in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

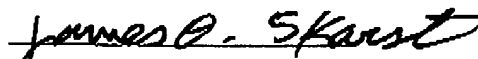
**III. Conclusion**

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: March 14, 2005

Respectfully submitted,



James O. Skarsten  
Reg. No. 28,346  
Yee & Associates, P.C.  
P.O. Box 802333  
Dallas, TX 75380  
(972) 385-8777  
Attorney for Applicants